Applications

Personal information privacy: implications for MIS managers

Sandra C. Henderson, Charles A. Snyder*

Department of Management, College of Business, Auburn University, 415 W. Magnolia, Auburn AL 36849, USA

Received 23 April 1998; revised 14 January 1999; accepted 20 March 1999

Abstract

Recent media attention to information privacy issues has shown that citizens are increasingly concerned about information privacy and their right to it. Governmental and other organizations have been collecting data about individuals at an increasing and, to many, alarming rate. The ability to gather so much information on individuals is largely because of advances in information technology (IT). It is important for IS managers and professionals to understand the issues surrounding personal information privacy in order to protect the rights of those from and about whom they collect data. A model is presented to provide managers guidance in dealing with privacy policy. Taking a proactive stance against privacy invasion could help stave off government intervention in passing legislation to create tighter controls over what can be done with an individual’s personal data. © 1999 Elsevier Science B.V. All rights reserved.

Keywords: Personal information privacy; Information privacy; Personal data; Privacy; Ethical issues; Right to privacy; Privacy policy

1. Introduction

Privacy is a fundamental right recognized in the United Nations Universal Declaration of Human Rights, the Council of Europe’s Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, the International Covenant on Civil and Political Rights, and many other international and regional treaties. Privacy has been defined as the ‘right of individuals to control the collection and use of personal information about themselves.’ The right to privacy has become one of the most important ethical issues of the information age [19].

Nearly every country in the world recognizes the right to privacy in their constitutions or laws. While some only provide provisions for such rights as inviolability of the home and secrecy of communications, many recently written constitutions, such as South Africa’s and Hungary’s, include specific rights to access and control one’s personal information. In many countries such as the United States, Ireland, and India where privacy is not explicitly recognized in the constitution, the courts or new laws have identified the right to privacy. In addition, international agreements that extol the right to privacy, such as the International Covenant on Civil and Political Rights or the European Convention on Human Rights, have been adopted into law by many countries.

Privacy, as a right, has roots deep in history. Evidence of the protection of privacy — with a focus on the right to solitude — can be found in early Hebrew culture and ancient China. Other cultures have recognized the right of privacy as a formal concept for centuries: the Greek ‘contumelia,’ the Roman ‘injuria,’ the German ‘Personlichkeitsrecht,’ the Swiss...
‘Geheimsspare,’ and the French doctrine of ‘la droit de la personnalite.’ The English allowed limited protection only if a collateral property right or breach of a confidential relationship was involved [16].

Privacy laws can be traced as far back as 1361 when the Justices of the Peace Act in England provided protection from peeping Toms and eavesdroppers. During the following centuries, several countries developed privacy laws. The Swedish Parliament enacted the Access to Public Records Act in 1776. This Act required that all government-held information be used for legitimate purposes. In 1792, the Declaration of the Rights of Man and the Citizen proclaimed that private property was inviolable and sacred. Stiff fines were invoked in 1858 as France prohibited the publication of private facts about individuals. In 1890, American lawyers Samuel Warren and Louis Brandeis published a paper that quoted Judge Thomas Cooley’s claim that the individual has ‘the right to be let alone.’ At this point, the whole issue of the right to privacy was the direct result of technology and lifestyle, thereby prompting the rather stinging commentary by Warren and Brandeis: “Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices that threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the house-tops’” [32].

The 1948 U.N, Universal Declaration of Human Rights provided a modern privacy benchmark. Article 12 states: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, not attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks” [31]. Similar provisions can also be found in Article 8 of the 1950 Convention for the Protection of Human Rights and Fundamental Freedoms. From this Convention, the European Commission of Human Rights and the European Court of Human Rights were created to oversee the enforcement of privacy rights. The American Convention on Human Rights Article 11 defines the right to privacy in a manner similar to the Universal Declaration. In 1965, the Organization for American States called for the protection of privacy in the American Declaration of the Rights and Duties of Man.

The advent of information technology (IT) increased interest in the right of privacy issue in the 1960s and 1970s. Largely due to increased surveillance potential and record-keeping abilities of computer systems, laws governing the collection and handling of personal information were demanded. In 1970, the first data protection law in the world was enacted in the Land of Hesse in Germany. National laws soon followed in several countries: the Swedish Data Act of 1973, the United States Privacy Act of 1974, the 1978 Austrian Datenschutzgesetz (DSG), the 1977 German Federal Data Protection Act (BDSG), the Danish Private Registers Act of 1978, and the 1978 French Act on Data Processing Data Files and Individual Liberties [22].

At the international level, two crucial instruments evolved in the 1980s: the Council of Europe’s (COE) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the Organization for Economic Cooperation and Development’s (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data. The rules contained within these two documents call for the protection of personal information at every step, from collection to storage and dissemination. Individuals also have the right to access and correct or amend their data [7, 23].

Over 20 countries have adopted these documents as the core as their data protection laws [14]. Based on Article 5 of the COE Convention, personal information must be:

- obtained fairly and lawfully;
- used only for the original specified purpose;
- adequate, relevant and not excessive to purpose;
- accurate and up to data; and
- destroyed after its purpose is completed.

A renewal of the interest in information privacy occurred in the late 1980s as a result of increased database marketing and telemarketing [8]. During this period, many more countries around the world adopted data protection laws. Information privacy issues remained at the forefront of consumer concern into the 1990s. This attention has been brought about by the increasing impact of IT on daily life [28] and by recent media attention. As evidence of the renewed interest, articles have appeared in newspapers and magazines. Television shows have included exposés
involving loss of personal data, and books have been published on privacy. All have contributed to the growing concern about information privacy. However, perhaps the major impact on information privacy and data protection concerns in many countries will come from the two European Directives that provide their citizens with a wider range of protection of their data.

In 1995, the European Union adopted the Directive on Data Protection designed to establish minimum standards for the processing and use of personal data. There were two reasons: (1) to ensure protection of the ‘fundamental right’ to privacy with respect to the processing of personal data, and (2) to prevent restriction of the ‘free flow of personal data’ among EU Member States on grounds of privacy protection [9]. The Telecommunications Directive was adopted by the Council and Parliament of the European Union in 1997. This Directive provides for protection to ensure the “fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the telecommunications sector” and to ensure free movement of data, telecommunications equipment and services among Member States [10].

Consumer attitudes about information privacy, concurrent with the increased media attention and the European Union Data Protection Directive, have brought about a significant increase in the potential legal liability for misuse of an individual’s personal information [29]. Organizations are being held liable for the improper use of information technology and personal information. Therefore, organizations need to be constantly aware of the issues surrounding personal information privacy and any repercussions that can occur if they do not take precautions to protect the information they collect on individuals. This paper presents a normative model designed to aid information system (IS) professionals and managers protect the personal information of their customers and other individuals.

IS professionals and managers should be aware of information privacy issues — especially the potential impact on existing IS and on future systems development. IS managers have the oversight responsibility for information liability as they have the most extensive knowledge of their organization’s systems and programs, and an intimate understanding of the data [27]. However, in order to perform this oversight function effectively and to provide justification for increased information security to policy makers, IS managers and professionals must understand the driving forces surrounding individuals’ concern about personal information privacy.

2. Driving forces

There are three main forces driving the growing focus on personal information privacy: (1) new technological capabilities; (2) increasing value of information; and (3) confusion surrounding the definition of what is ethically right and what is wrong [20].

2.1. Technological capabilities

Highly sophisticated technology with its enhanced capacity for communication, computation, storage, and retrieval has given personal information privacy and the right of privacy new meaning [12]. In the 1950s, when documents were kept in filing cabinets, control over the information was relatively easy to maintain, because physical access to files could be limited by the use of locks and guards. As computerization increased, more documents were stored on magnetic media, making the provision of security a greater problem. In the 1990s, documents can still be filed in filing cabinets, but most are stored on electronic media and transmitted over networks in an electronic format. As organizations rely more on electronic communication, there is increased concern that privacy will be harder to maintain. The main threats include computer matching, hackers seeking passwords or the challenge of breaking a security code, corrupt or careless medical records clerks, insurance companies accessing medical records, busybodies in hospitals, e-mail monitoring, and electronic surveillance [26, 30].

The proliferation of Enterprise Resource Planning (ERP) and client–server systems has allowed organizations to pull data from a number of internal and external sources. The ability to cross-correlate and share information is now relatively easy and cheap. These capabilities come at a high price for personal information — an increased threat to an individual’s privacy. Control over personal information is lost and any data errors are exacerbated as the data move from one computer to another.
New developments in computer technology have enabled organizations to downsize and distribute their computing platforms. Applications once run on mainframes can now run on PCs with data stored on the individual hard disk drives and on LAN file servers. Use of corporate Intranets has also become widespread and data control has become more difficult. The trend toward decentralization has contributed to the threat to personal information privacy, mainly because it is harder to manage data and keep tight control when it is spread out over several computers.

2.2. Increasing value of information

As computing and data management continue to become more decentralized and control is diffused, the value of information is increasing with new ways of using it for strategic and competitive advantage. Organizations have found that the data collected about customers can be used to target prospects, improve customer satisfaction and retention, and identify opportunities for new products or services. For instance, companies are increasingly targeting certain consumer segments instead of all potential buyers. In order to do this, companies need to know specific purchasing characteristics of individuals. Therefore, it is necessary to store and share information with other organizations — usually without user knowledge or permission. The ability to gather this information, often from several sources, is made possible because of increased processing speeds and decline in storage costs. The use of such capabilities for this unauthorized secondary use of personal information has caused the largest outcry from the public about personal information privacy violations. However, Hagel and Rayport [15] suggest that this outcry is more the result of consumers becoming aware of the value of the information that they have freely divulged in the past.

3. Rights of information privacy

According to Branscomb [4], “privacy law consists primarily in the protection of that private space surrounding one’s person into which outsiders should not be permitted to penetrate. Its origins date back to common courtesy and social more that respected the need for private spaces.” Currently, privacy laws in the United States and many other countries do not provide the protection of, for instance, the European Union. For example, the U.S. Privacy Act of 1974 offers only protection against data held in government databases about U.S. citizens. Where does this leave the protection an individual’s personal data from private sector organizations in the United States?

For the most part, private organizations are exempt from privacy legislation with the exception of the Fair Credit Reporting Act of 1970, the Family Educational Rights and Privacy Act of 1978, the Privacy Protection Act of 1980, the Cable Communications Policy Act of 1984, and the Video Privacy Protection Act of 1988. The main limitations of these laws is that enforcement is entirely in the hands of the individuals who must recover damages in court. Thus, privacy laws do not protect privacy well and, in fact, are far behind the developmental trajectory of information technology [18].

4. Privacy policy

The publicity surrounding privacy issues has led to some action. “Our awareness has been raised; our
resistance, increased. We must act with vigor and vigilance to ensure our privacy, for it is a right that affects every individual with an identity and a personal history’’ [11].

Despite privacy laws that have been enacted in many countries, there is still a need to develop national privacy policies that address: the balance between the right to privacy and the right to access; the expectations of individuals and the needs of society; the appropriate level of privacy protection that should be afforded to public figures, private persons, governments and other organizations; clear guidelines as to what information an individual can be compelled to reveal to benefit society and what should be under his or her control [33]. However, privacy policies are notoriously weak — often reading more like a simple disclaimer. According to Rotenberg [25], “The essential framework for privacy protection — a code of fair information practices, setting out the obligations of companies that collect personal information and the rights of individuals that give personal information — is often missing, incomplete or unenforceable.” As an alternative to government regulation, industries and individual organizations should consider other methods.

5. Self-regulation and policy

Self-regulatory policies and procedures may be a way to handle information privacy issues. The Association for Computing Machinery (ACM) has included a section on privacy in its Code of Ethics and Professional Conduct. Their code states that “It is the responsibility of professionals to maintain the privacy and integrity of data describing individuals. This includes taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals” [1].

The importance of having adequate policies in effect is hard to overestimate. An example of loose policy was the U.S. Internal Revenue Service (IRS) revelation of sensitive private data from taxpayer records in response to telephone inquiries for which the caller only had to provide name, social security number, and address. In an investigation, the IRS found that their auditors (and other individuals) could easily secure tax and income data without the IRS verifying the caller’s true identity. The manager of any organization, public or private, with databases containing sensitive personal data should establish adequate policies and ensure that they are properly promulgated to those workers who have responsibility for the protection of privacy. However, one potential problem with this concept or any other privacy rule or standard is enforcement: Who decides what privacy rules, laws, or standards apply to any given situation? Who enforces these rules or codes [13]?

Four principles should be followed in data collection: (1) data should be collected on individuals only to accomplish a legitimate business objective; (2) data should be adequate, relevant, and not excessive in relation to the business objective; (3) data should be obtained in a lawful manner; and (4) individuals must give their consent before data pertaining to them can be gathered — such consent may be implied from the individual’s actions. Four principles also apply to data accuracy to ensure that misleading information will not be distributed: (1) sensitive data gathered on individuals should be verified before it is entered into the database; (2) data should be accurate and, where necessary, kept up to date; (3) the file should be made available so that the individual can ensure that the data are correct; and (4) if there is a disagreement about the accuracy of the data, the individual’s version should be noted and included in any disclosure of the file. In order to ensure data confidentiality: (1) computer security procedures should include physical, technical, and administrative security measures; (2) third parties should not be given access to data without the individual’s knowledge or permission, except as required by law; (3) disclosures of data, other than the most routine, should be noted and maintained for as long as the data are maintained; and (4) data should not be disclosed for reasons incompatible with the business objective for which it was collected [2].

Whether governments enact more privacy laws or organizations follow self-regulation, IS managers and general managers need to implement controls to ensure that the information collected is done so in a manner that protects the individuals’ personal information privacy. Several issues should be addressed by both managers to ensure they are knowledgeable about the latest developments in information privacy.
6. Implications for managers

Careful consideration of the implications of personal information privacy issues should be a priority in organizations. Conscious and deliberate decisions must be made by upper management on the operation, control, and management of information services [17]. Managers should identify any potential underlying privacy-related problems and be prepared to take corrective actions and appropriate measures to protect the individual’s privacy. Table 1 contains a normative model that could be embraced by organizations who are concerned about privacy issues and are ready to take a stance to help ensure individuals’ rights to privacy.

Managers need to be aware of new developments. One person should be designated responsible for information liability and to maintain a close connection with functional area managers. This practice would help ensure that privacy policies are maintained and legislation monitored and that the information reaches the appropriate personnel. Close contact with the functional area managers would help the designated person keep up with the organization’s practices concerning personal information. Currently, there is a need for IS managers to take a proactive stance regarding information privacy management issues. If they do not do so, levels of concern about information will continue to rise and citizens will look to the government for solutions [21]. While there is not necessarily anything wrong with government intervention, in many industries self-regulation works better.

IS managers need to think through potential information problems within their firms and take action to reduce the risk that their information systems might be used to invade an individual’s privacy. There are several areas in which IS managers should be particularly cautious. First, an organization does not need to store information that it does not need nor information that could cause public backlash. Second, information should be used for the purposes for which it was collected or for which individuals believe it was collected. Third, if information is shared electronically, the organization should have approval of the individuals concerned or knowledge that the individuals would approve of the sharing. Next, proper human judgement should be used in making decisions concerning an individual’s personal information. A manager should also be cautious when pieces of personal information are pulled from different sources to make a more complete file. Finally, internal controls and procedures should be in place to prevent and/or correct any errors in an individual’s personal information.

IS managers also need to take into consideration the following points: access to data should be limited to only those who actually need access to the data, and hard copy and oral data need to be protected just as much as computerized data [24]. An IS manager should also keep in mind the fact that individuals are less likely to perceive practices as privacy-invasive when (1) information is collected under the umbrella of an existing relationship; (2) they feel that they have control over future use of the information; (3) the information collected or used is relevant to the transaction; and (4) they believe the information will be used to draw reliable and valid inferences about them.

With the proliferation of data warehousing and data mining, the vulnerability of organizations to accusations of misuse of personal data is likely to increase. Most data warehouses re-orient data to have a customer focus. Some organizations have reported the

Table 1
A proposed normative model for privacy issues in the organization

1. Assume responsibility for personal information
   a. Designate one individual responsible for information liability
   b. Educate appropriate personnel on privacy policy
2. Map privacy sensitive data
   a. Identify databases with personal information
   b. Identify use of personal information
      (1) Applications requiring use
      (2) Applications not requiring use
      (3) Protection afforded an individual’s personal information
3. Ascertain extent of personal information
   a. Adequacy for business objective
   b. Relevance for business objective
   c. Non-excessive data collected for business objective
4. Ensure data sources and controls
   a. Lawful collection of personal information
   b. Accurate information in databases
   c. Verified information databases
   d. Promulgation of policy
5. Disclose information to individuals concerned
   a. Resolve in favor of individuals
   b. Assure security of data
   c. Obtain permissions for internal and third-party use
6. Document use
   a. Record all disclosures and purposes (provide an audit trail)
   b. Designate responsible managers
7. Take action to limit damage if procedure breaks down
ability to provide detailed personal data profiles for their customers so that individuals can become market segments of size one. Thereby, one long distance provider is said to have greatly increased the effectiveness of its telemarketing efforts to reduce loss of its most valuable customers. The ability to amass personal data from multiple sources and generate ‘intimate’ customer profiles is likely to lead to widespread deployment of such systems. Managers contemplating such moves must be sure that they implement policies to protect the personal data they wish to exploit or tell their staffs that they are likely to face stiff rebuke and penalties if the data are misused.

A proactive stance against personal privacy invasion could help prevent tighter and possibly onerous legislation aimed at protecting individuals. With the U.S. government’s inept handling of previous legislative attempts to control the proliferation of personal information available due to information technology, self-regulation either by the industry or individual organization could be the best answer. When individuals have had enough of privacy-invasion issues, such as their personal information being massaged by too many computers without their consent, governments worldwide will be forced to deal with the issue by enacting further legislation that will require the consent of individuals before marketing information about them.

Another twist to this complex issue deals with individuals becoming increasingly aware of the value of their personal data. Currently, organizations collecting personal data about individuals appear to have the power of ownership of the data. However, individuals may soon reclaim ownership of their data and demand value — in the form of better service or even cash — in exchange for it [5]. This could have a major impact on the cost of collecting and maintaining consumer data. Protecting individuals’ privacy can help ensure the continued willingness of individuals to share their information. According to Bresnahan, ‘privacy protection pays’ because ‘indifference can get you in trouble’ [6].

References

Sandra C. Henderson is a doctoral student of Management Information Systems in the Department of Management at Auburn University. She holds an Master’s of Accountancy with a concentration in Accounting Information System from Florida State University. She received a B.S. in Accounting from Albany State University. Previously, she worked as a controller and IS coordinator for a light manufacturing plant. Her current research interests include information privacy, transborder data flows, and database systems development. She has presented at the SAIS conference.

Charles A. Snyder is the Woodruff Endowed Professor of Management (MIS) in the Department of Management at Auburn University. He received a Ph.D. in Management from the University of Nebraska. He holds an MS in Economics from South Dakota State University, an MBA from Ohio State University, and a BFA from the University of Georgia.


He has extensive management, research, and consulting experience. His research interests include knowledge management, information resource management, expert systems, computer-integrated manufacturing, systems analysis and design, and telecommunications management. Dr. Snyder is a member of SIM, DSL, ACM, IEEE, IRMA, AIS, SAIS, and other major professional societies. He is the past President of the Alabama SIM and the Southern MIS Association. He is currently a member of the Society for Information Management working group on knowledge management and is Alabama representative to the International organization. Dr. Snyder has consulted to such firms as AT&T, BellSouth, South Central Bell, TRW, Coors, and software companies. He serves as a director of five organizations. Before his academic career, he served for 20 years in a variety of operations, staff, and command positions as an officer in the USAF.